Alessandro Banzer

February 23, 2014 | 2 minute read

Mitigating Control Lifecycle

20 16 12,444

A high amount of time during a SAP GRC project will be spent on defining processes and responsibilities. My suggestion is to think in lifecycles for getting a better understanding of the processes and who is taking over the responsibilty.

In this post I would like to clarify the lifecycle of Mitigating Controls. I have grouped them into four steps Create, Change, Delete and Review. Please see for each step expected Tasks and who is involved.

On request from Colleen I have additionally added the RACI matrix to see who is **R**esponsible, **A**ccountable, **C**onsulted and **I**nformed for each step. Please be aware that this is very much depending on the point of view and can be different in your organization. My considerations are commonsense and pretty much of thinking in smooth processes throughout a global enterprise.

Creation of Mitigating Controls

Tasks
Define the control including:

- Control description
- Control execution
- Control approver and control monitor
- Documentation of control execution
- Reports used to monitor the risk

Involved functions

- Control Owner
- Internal Control responsible
- SAP GRC responsible

Creation of Mitigating Controls

	Control owner	Internal Control responsible	SAP GRC responsible
Control description	I	A	R
Control execution	I	A	R
Control approver and control monitor	I	A	R
Documentation of control execution	R	A	
Reports used to monitor the risk	R	A	

Changing of Mitigating Controls

Tasks

Change the control for example:

- Control description
- Control execution
- Control approver and control monitor
- Documentation of control execution
- Reports used to monitor the risk

Involved functions

- Control owner
- Internal Control responsible
- SAP GRC responsible

Changing of Mitigating Controls

	Control owner	Internal Control responsible	SAP GRC responsible
Control description	I	A	R
Control execution	I	A	R
Control approver and control monitor	I	A	R
Documentation of control execution	R	A	
Reports used to monitor the risk	R	A	

Deletion of Mitigation Controls

Tasks

- Delete the mitigating control within SAP GRC AC
- Document the decision of deletion of the mitigating control

Involved functions

- Control Owner
- Internal Control responsible
- SAP GRC responsible

Deletion of Mitigating Controls	Control owner	Internal Control responsible	SAP GRC responsible
Delete the mitigating control within SAP GRC AC	I	A	R
Document the decision of deletion of the mitigating control	C	R	

Reviewing of Mitigating Controls

Tasks

- Analyse if maintained controls within SAP GRC are still valid
- Analyse if the mitigating controls are covering the risk fully
- Test the effectiveness of the mitigating controls

Involved functions

- Control owner
- Internal Control responsible
- SAP GRC responsible

Reviewing of Mitigating Controls	Control owner	Internal Control responsible	SAP GRC responsible
Analyse if maintained controls within SAP GRC are still valid	R	A	C
Analyse if the mitigating controls are covering the risk fully	R	A	
Test the effectiveness of the mitigating controls	R	A	

If you want to have further information or contribute in this blog post do not hesitate to contact me or reply to this post directly.

Follow

Like

RSS Feed

Alert Moderator

Assigned Tags

SAP Access Control

governance risk and compliance sap grc

grc

mitigating control

Similar Blog Posts

SAP GRC 10.0/10.1/12.0 - Creation of Mitigation Controls

By Madhu Babu #MJ Jan 17, 2014

ARA - For the new kid on the block

By S A Aug 27, 2014

Mitigation Controls creation and assignment in SAP GRC 12.0

By Javed Khan Apr 19, 2023

Related Questions

Error while setup of new SOD Mitigation Control

By Piyush Nandan Feb 26, 2021

SAP GRC Access Control: Rule Set Transport and Generate, and Mitigation Control Assignment

By Reza Ahoui Oct 07, 2020

SAP GRC Access Control: Suggestion for Mitigating Control Naming Convention

By Reza Ahoui Jul 14, 2020

20 Comments

You must be Logged on to comment or reply to a post.

Former Member
February 24, 2014 at 11:51 am

thanks for this very valuable input, alessandro. i will use in my projects.

Like 0 | Share

Colleen Hebbert
February 24, 2014 at 10:20 pm

Hi Alessandro

Great to see someone like you starting up blogs around process and governance of using GRC. It helps to better understand why GRC has been built the way it has and how to go about designing your processes.

Would it be possible to expand this out to capture your acronyms (e.g. ICS) and a high level summary of why they should be involved in the decision making (possibly a RACI model); what sort of activities and impacts they should consider in determining the control.

Regards

Colleen

Like 0 | Share

Alessandro Banzer | Blog Post Author
February 25, 2014 at 2:10 am

Dear Colleen,

thank you very much for your input which is much appreciated.

For sure I will update my blog to get a clear understanding for everyone. For someone like me, who is working with such terms daily, everything is naturally and I do not realize that I am writing in technical jargon.

Best regards,

Alessandro

Like 0 | Share

Colleen Hebbert
February 25, 2014 at 2:12 am

Hi Alessandro

We are all guilty of using technical jargon or client/business specific terms that can have different meanings elsewhere.

Cheers

Colleen

Like 0 | Share

Arif Mahamud
February 25, 2014 at 4:50 am

Thanks Alessandro really good

Like 0 | Share

Alessandro Banzer | Blog Post Author
February 25, 2014 at 5:25 am

Tanks a lot! Hope you can use this in your projects.

Like 0 | Share

Former Member
February 25, 2014 at 5:09 am

Hi Alessandro,

This is really quite a ahelpful document.

Could you please elaborate on "templates used to monitor the risk" and do you mean ICS by some Audit-controls?

Like 0 | Share

Alessandro Banzer | Blog Post Author
February 25, 2014 at 5:27 am

Hi Ameet,

thanks for your feedback.

This was a mistake and I corrected already in the latest version. Templates used are the reports which can be defined for monitoring the risk.

ICS is an internal jargon we are using for "Internal Control System". I've changed as well to "Internal Control responsible" and hope this makes it more clear.

Thanks and regards,

Alessandro

Like 0 | Share

Former Member
February 25, 2014 at 8:01 am

Hi Alessandro,

Thank you for clarifying my doubts!!

Now, I am clear with templates/reports to monitor the risk.

Thanks,

Ameet

Like 0 | Share

Former Member
February 25, 2014 at 8:00 am

Hi Alessandra,

That's a good overview!

Could you share who is generally playing each function you mentioned.

For intance, who is the control owner, the internal control responsible, the SAP GRC responsible ?

In our company, we are using SAP GRC 10 and the control owners we put for each mitigating control (MC) are our internal auditors. They are also mentioned as monitor.

However, the controls that are linked to the MCs are supposed to be executed on a regular basis (monthly mosto f the time) by the manager or designed person for the respective users assigned to the MC. Therefore, when our internal auditor are doing their audit they are asking for evidence that the control was processed as expected.

We, as GRC admin, are doing MC assignment removal when a user doesn't have any risk anymore due to roles assingment change or role content change. We are also proposing roles removal options to remove a MC from a user when that user didn't execute the set of Tcodes generating the risk. We are also maintaining and supporting the whole Access Control application (workflows, risks, functions, ...). Is the SAP GRC responsible related to our GRC Admin as described above ?

Thanks in advance for your feedback.

Feedback from anyone else is also welcomed.

Patrick.

Like 0 | Share

Alessandro Banzer | Blog Post Author
February 25, 2014 at 9:52 am

Hi Patrick,

thanks for your feedback. I try to clarfiy all your questions and hope it helps for a better understanding.

Regarding the ownership:

- Mitigation Control Owner is in our enterprise the ICS (Internal Control System) responsible from each entity. As we have different Internal Controls in different entities each entity has its own owner. To generalize this is definitely a business person in my point of view.

- Internal Control responsible we have separated into two levels. We have a global responsible who is also taking care of the GRC. Secondly, we have in each entity a local responsible who is taking care of the internal control system. When it comes to mitigation and defining compensating controls this is part of the local responsible. Mostly in close collaboration with the global counterpart.

- SAP GRC responsibilities we have splitted into two main areas. Business perspective and technical perspective where the business responsible for GRC is actually maintaining GRC (e.g. Create/Update/Delete mitigating controls, run risk analysis, etc. etc.). The technical counterpart is doing technical settings in the background (e.g. SPRO, rule set upload, MSMP workflows, etc. etc.).

From our current set up the Control Monitors are business functions which we have defined in the Internal Control System. Each function then gets a name from business (mostly process owners) and that is the one who is maintained as Monitor.

Our internal and also external auditors are reviewing and asking for evidence directly by the Control Monitor as it is his responsibility for his particular organization.

Mitigation Control removal, as you mentioned, are done by our business GRC responsible (from business itself) via the Invalid User Mitigation report.

Generally I am saying that the complete ownership of GRC must be in business and definitely not in IT. IT or a SAP Competence Center is only supporting business when it comes to technical aspects of GRC like updates, bug fixing, etc.

Hope to get also your opinion and thoughts on this.

Looking forward to hear from you.

Regards,

Alessandro

Like 0 | Share

Former Member
February 28, 2014 at 8:07 am

Thanks for sharing this helpfull info…

Regards

Samiran

Like 0 | Share

Pranjal Garg
February 28, 2014 at 11:16 am

This is awesome stuff.

Your way of explanation with the help of Graphs is good.

I like it

Like 0 | Share

Former Member
May 29, 2014 at 10:17 am

This is very useful. Thanks

Like 0 | Share

Former Member
October 16, 2014 at 10:45 pm

Once I have a mitigating control set up and it's being used to mitigate risks, how can I change the assigned mitigating control monitor (e.g., a new person assumes a job)? When I attempt to change the name in the control set-up, it's states the control is being used to mitigate risks and cannot be changed. GRC will allow me to add the desired name and save (I just cannot delete the old name). The only way I can figure to change the assigned monitor is run a report of mitigated risks, sort by the control in question, and then change each instance of mitigation one-by-one using the control and monitor drop-down menu. This takes forever. There must be an easier way to simply re-assign control monitors. Please advise. Thanks.

Like 0 | Share

Alessandro Banzer | Blog Post Author
October 22, 2014 at 6:46 am

Hi Scott,

thanks for your feedback. You should have a look on my other document Mass change of Mitigation Assignments which describes your problem in more detail.

Let me know if that helps.

Regards,

Alessandro

Like 0 | Share

Former Member
September 12, 2016 at 7:26 pm

Hi Alessandro,

Is there any document / standard GRC workflow for mitigating control assignments review and FFID assignment review like UAR.

Thanks

Narasimha.

Like 0 | Share

Former Member
December 26, 2014 at 5:24 pm

Hi Alessandro,

How Could i know my MItigation controls are active?Deafult is 365 day.is there any report shows validity of MItigation control

Like 0 | Share

Former Member
December 5, 2015 at 3:49 pm

Great Content. Are you aware of any standard GRC workflow we can use to periodically review mitigating controls and mitigating control assignments?

If not, how would you propose this could be done in a more efficient manner than manually!

Thx

Denis

Like 0 | Share

Former Member
June 28, 2016 at 11:12 am

Hi Alessandro,

Very helpful document !!

Regards,

Vinaya

Like 0 | Share

Find us on

Privacy	Terms of Use
Legal Disclosure	Copyright
Trademark	Cookie Preferences
Newsletter	Support